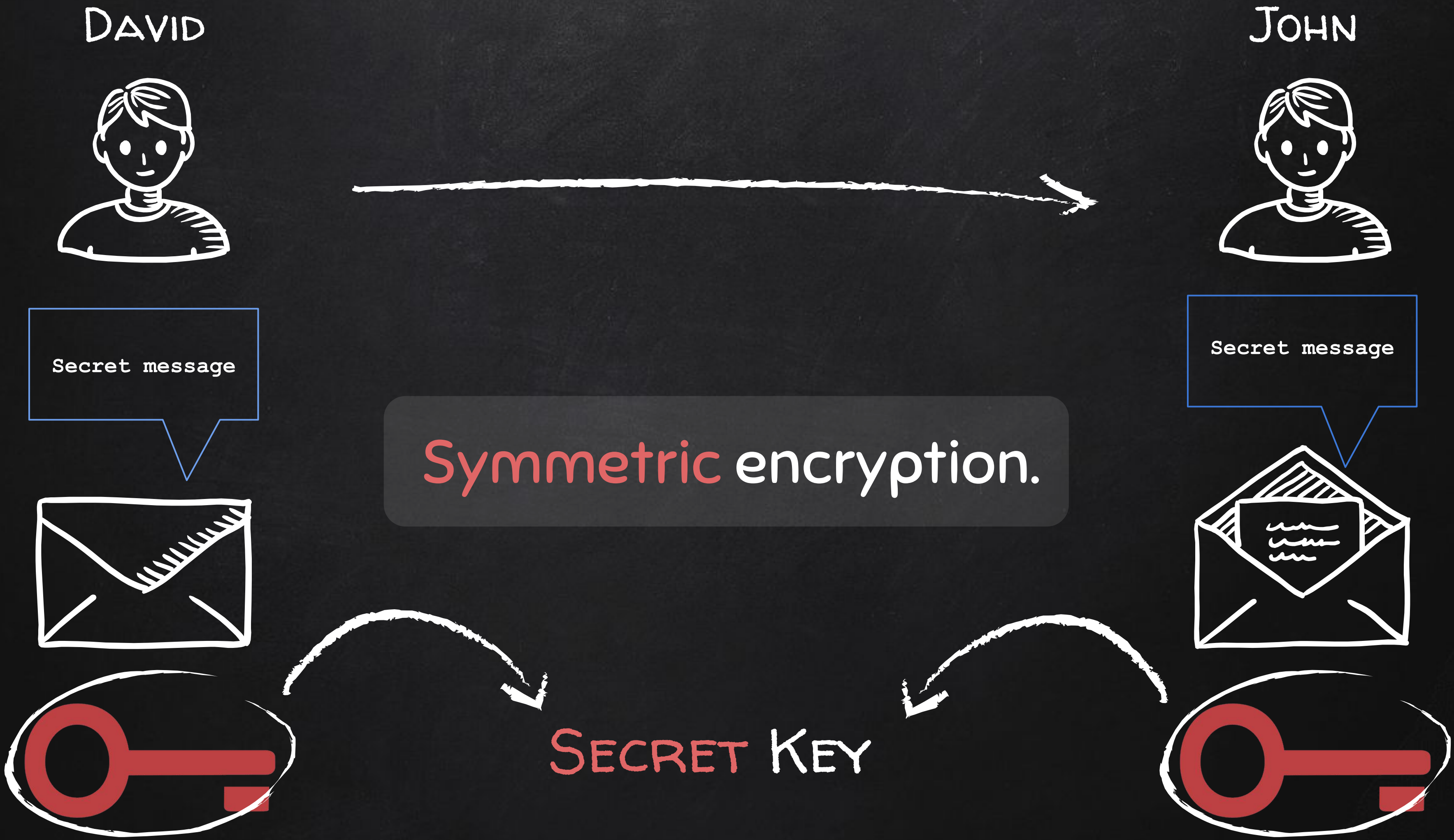
PGP - Pretty Good Encryption

- Very strong public key encryption.
- Unbroken.
- Encrypt emails, text or files.
- Sign message or files to verify integrity.



Symmetric encryption.

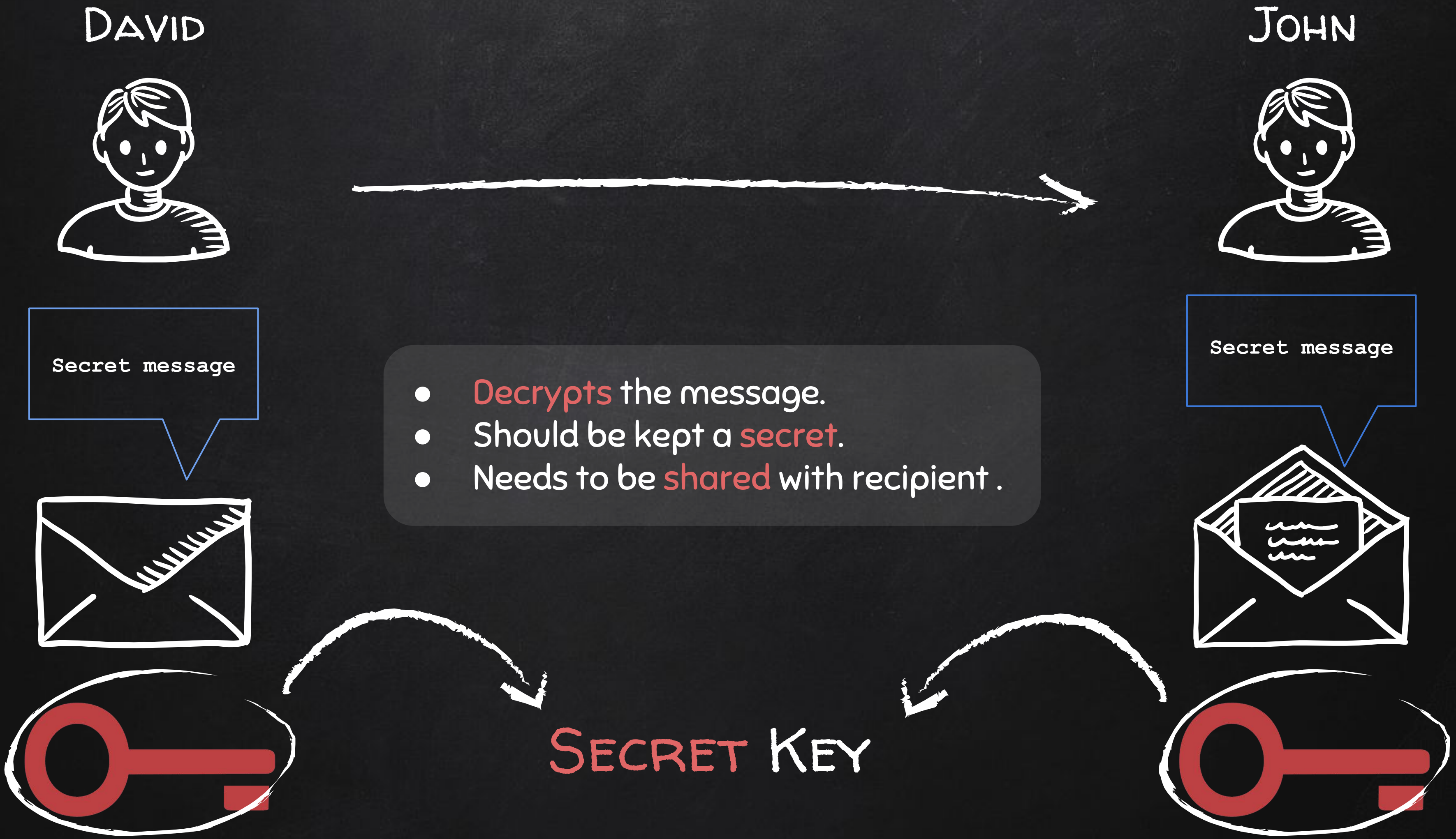
David

John

Secret message

Secret message

Secret Key



DAVID

JOHN

Secret message

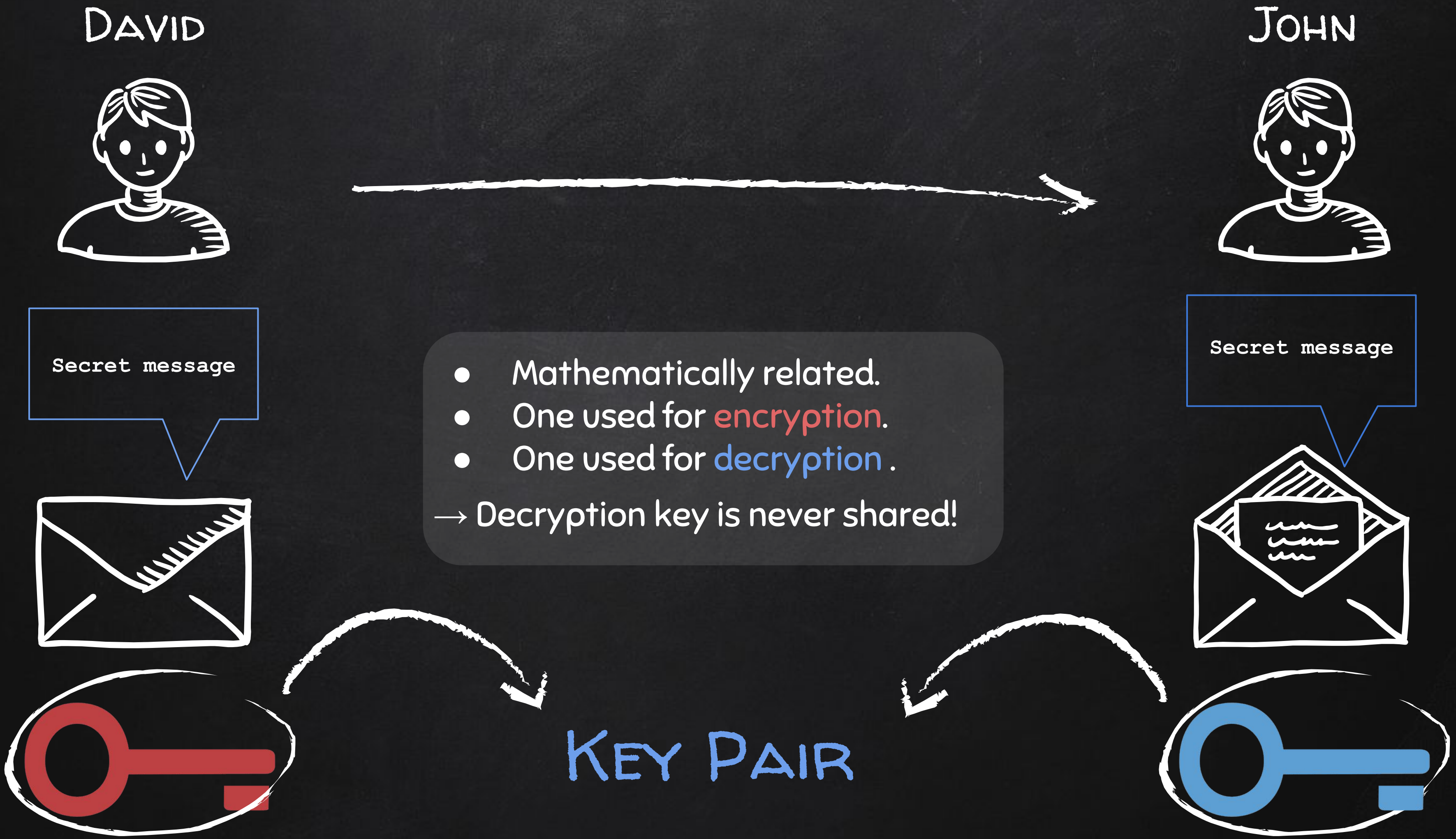
Secret message

- Decrypts the message.
- Should be kept a secret.
- Needs to be shared with recipient .

SECRET KEY

David
John
Secret message
Secret message

Asymmetric encryption.



David

John

Secret message

Secret message

- Mathematically related.
- One used for encryption.
- One used for decryption .

→ Decryption key is never shared!

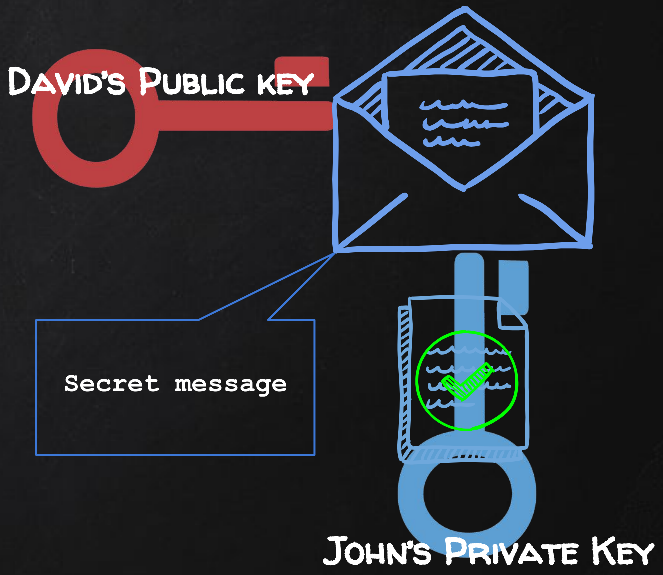
Key Pair

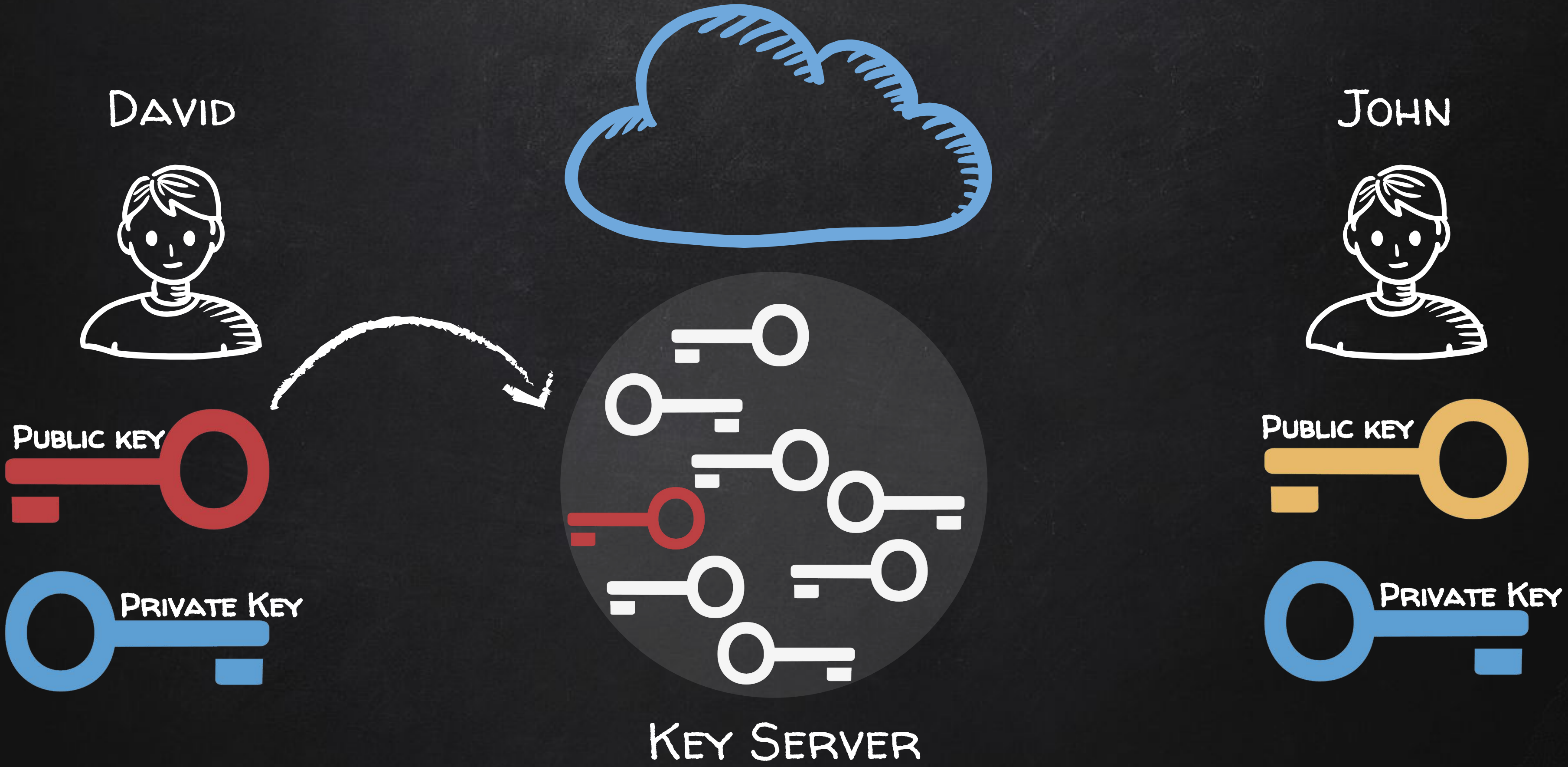
Sender (David):

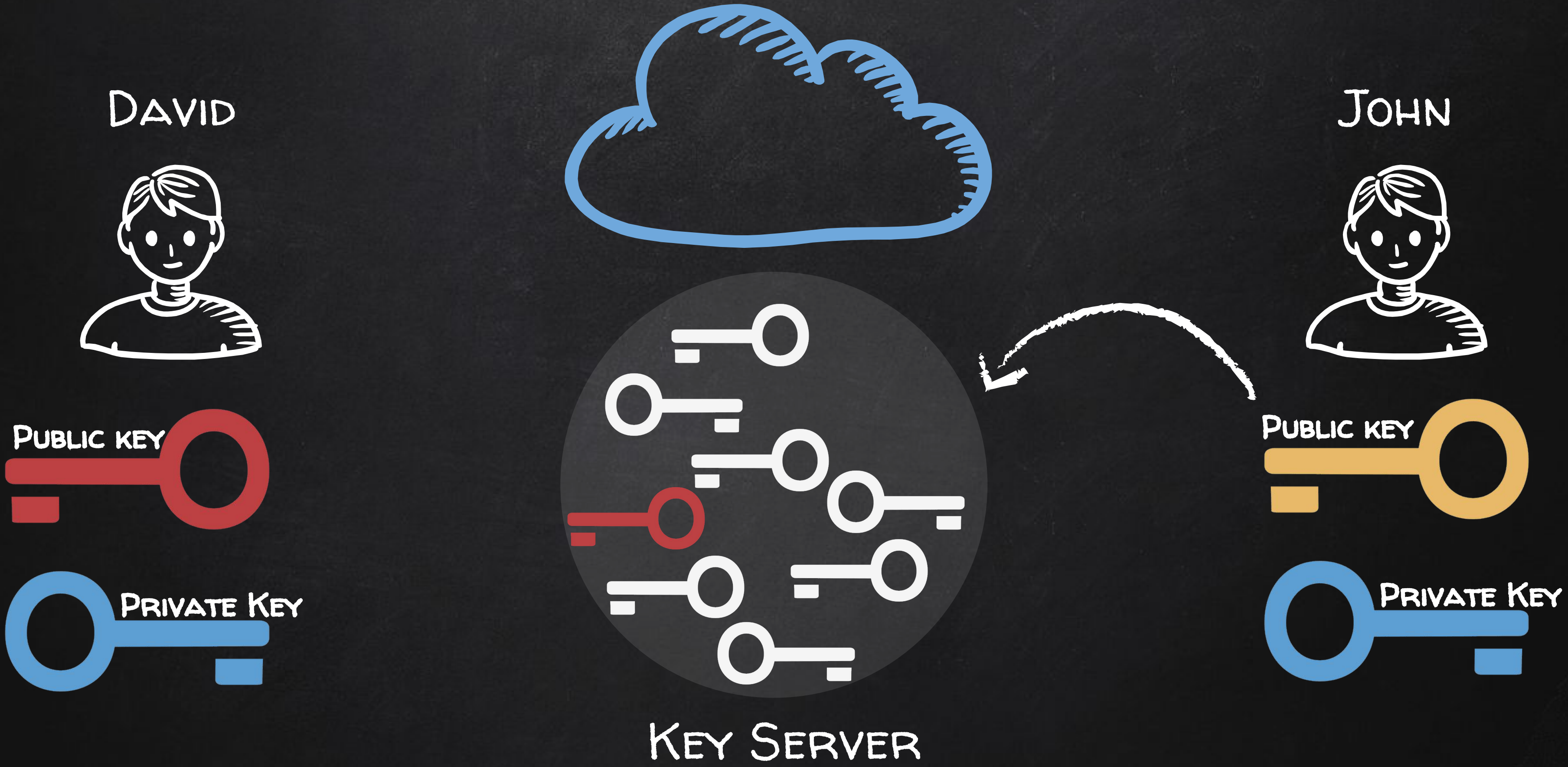
1. Encrypts message with receiver's public key.
2. Signes message with own private key.

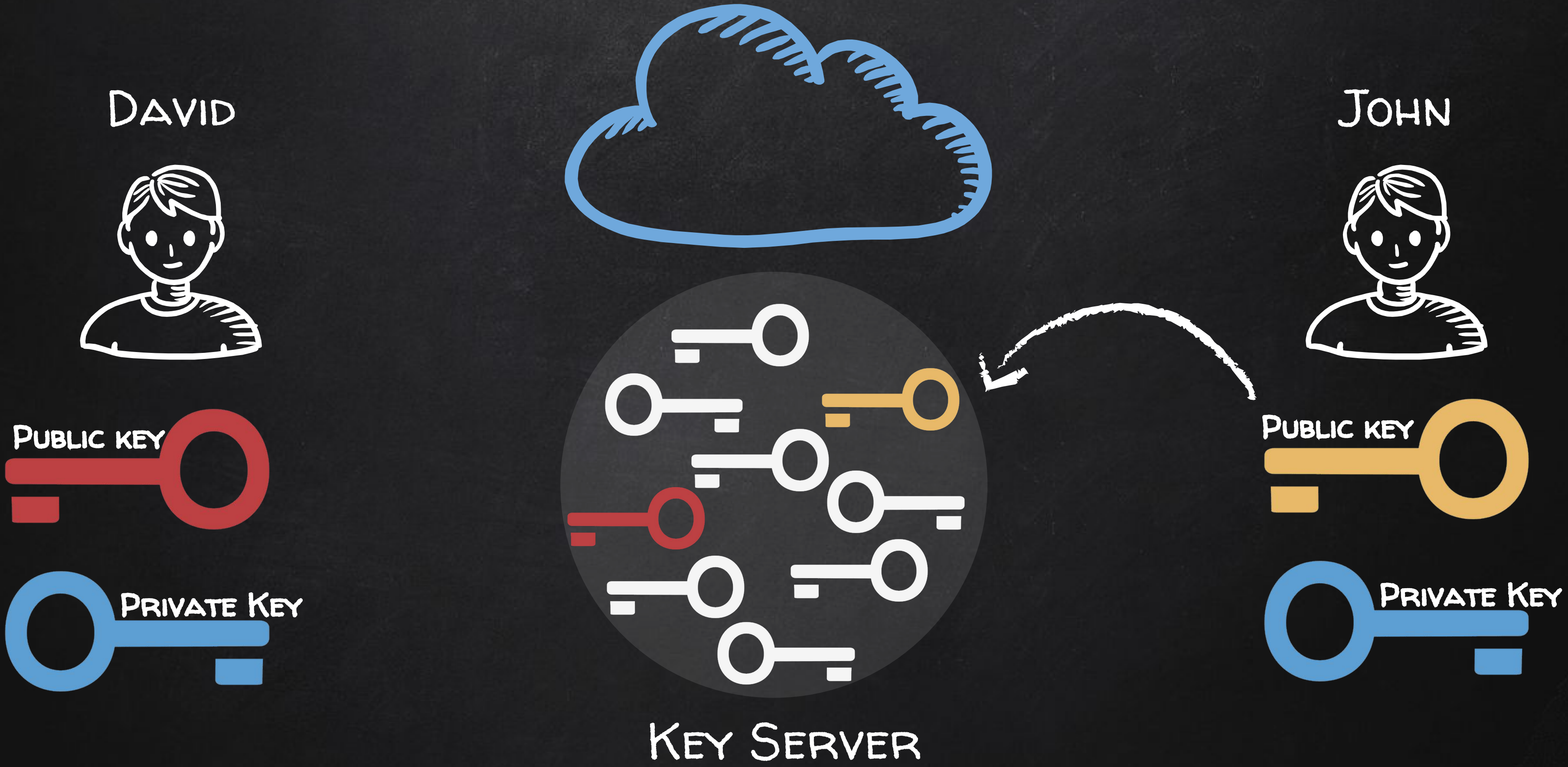
Receiver (John):

1. Verifies signature with sender’s public key.
2. Decrypts message with own private key.




David
John
Public key
Private Key
Public key
Private Key
Key Server


David
John
Public key
Private Key
Key Server
Public key
Private Key



David

John

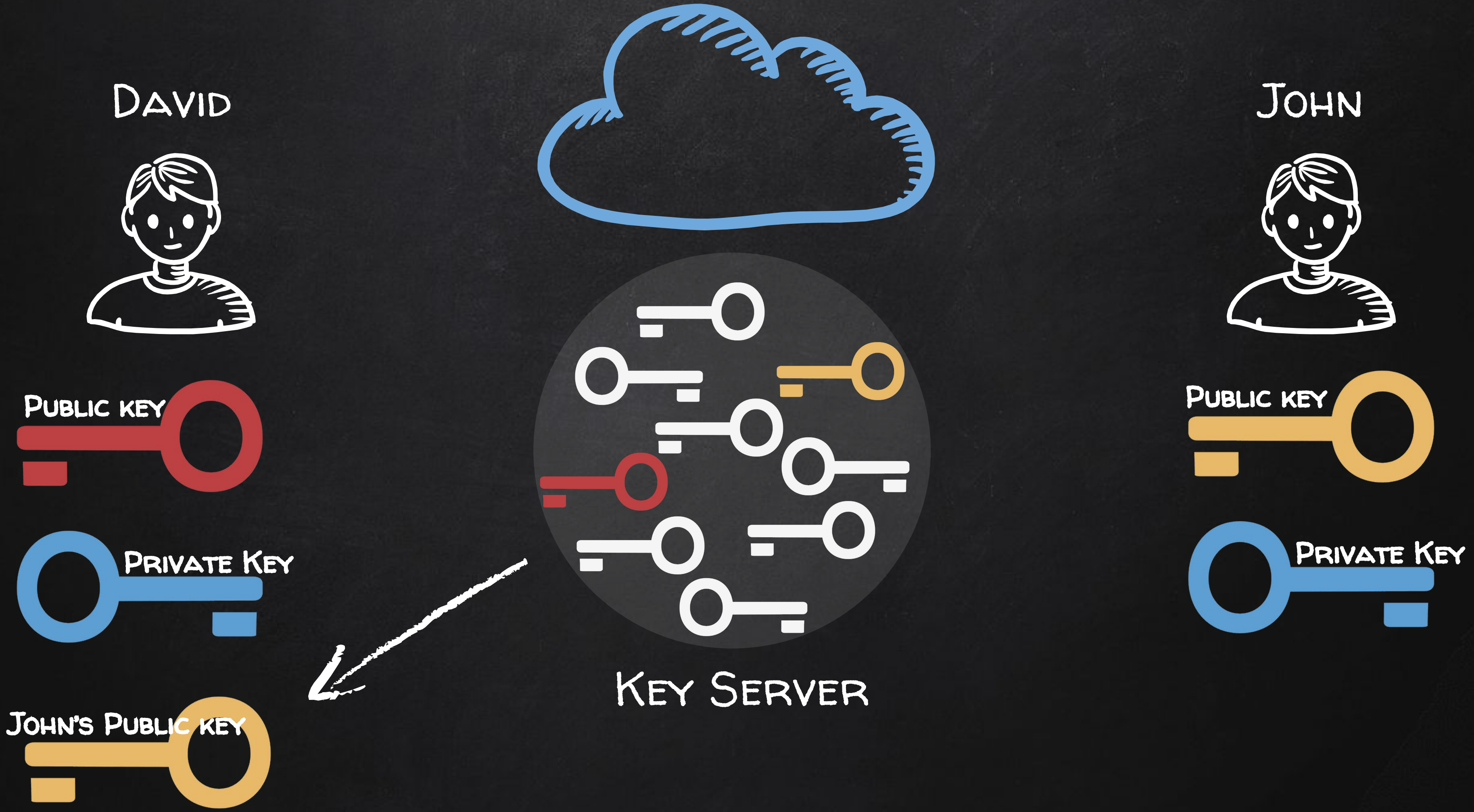
Public key

Private Key

Public key

Private Key

Key Server



David

Public key

Private Key

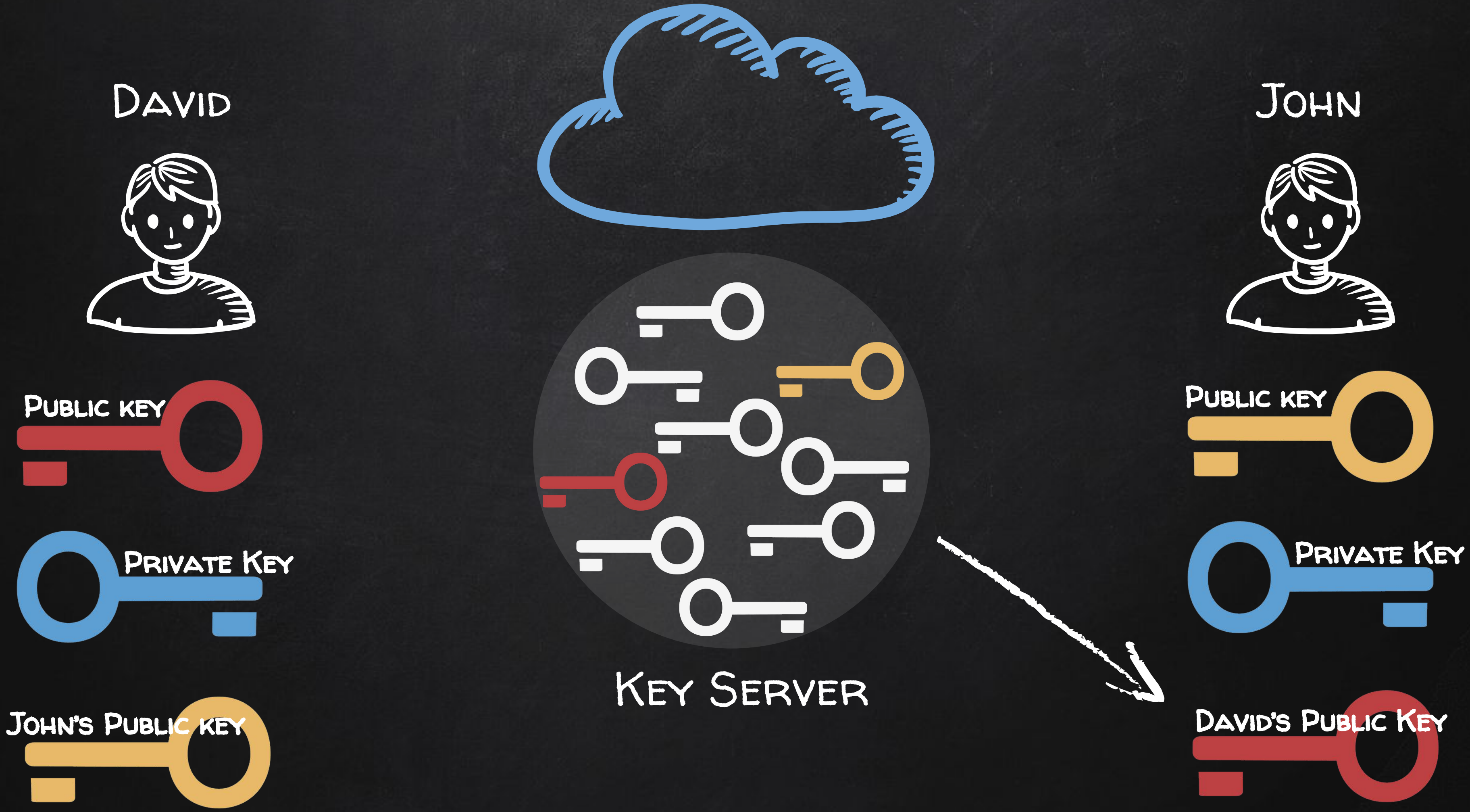
John's Public key

Key Server

John

Public key

Private Key



David

John

Public key

Private Key

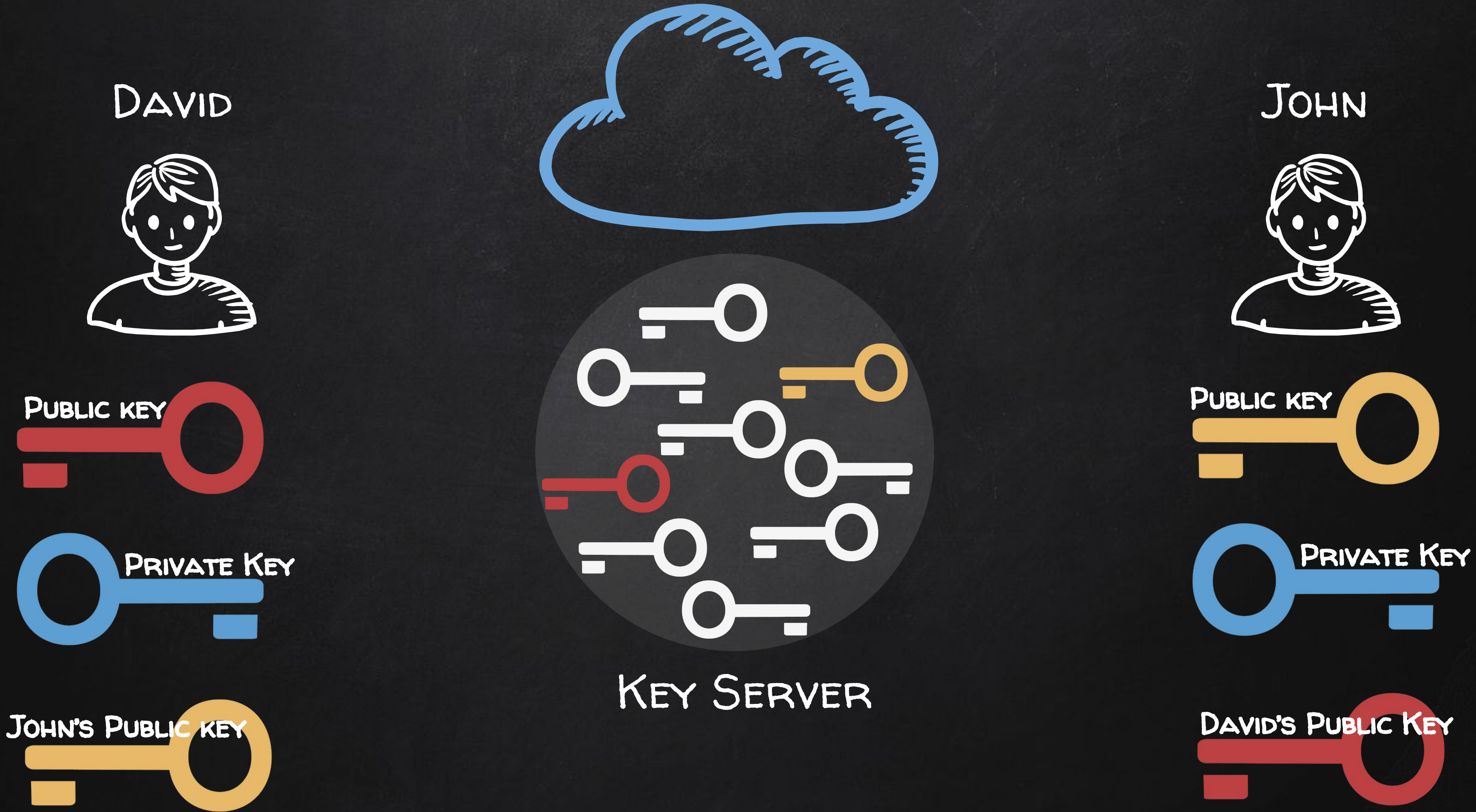
John's Public key

Key Server

Public key

Private Key

David's Public Key



David

Public key

Private Key

John's Public key

Key Server

John

Public key

Private Key

David's Public Key